REMARKS

The Office Action mailed March 21, 2007 has been reviewed and carefully considered. No new matter has been added.

Claim 1 has been amended. Claims 1-7 are pending.

Claims 1-7 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Diffie-Helman Key Exchange, Michael C. StJohns, Internet-Draft, 1998 (hereinafter "StJohns") in view of United States Patent No. 6,067,621 to Yu et al. in further view of SNMPv3: A Security Enhancement for SNMP, William Stallings, IEEE, 1998 (hereinafter "Stallings").

It is respectfully asserted that none of the cited references, either taken singly or in any combination, teach or suggest the following limitations of Claim 1:

> converting the shared secret into a readable password;
>
> converting the readable password into a secret key; and
>
> setting the initial authentication key and the initial privacy key to the value of the secret key,
>
> wherein each of said converting steps are independently performed by both the SNMP agent and the SNMP manager.

The wherein clause of Claim 1 is added by this amendment. Support for the same may be found at least at page 7, lines 16-26, and page 8, lines 14-23, which disclose the following (emphasis added):

> Next, in a preferred embodiment, the SNMPv3 agent converts the shared secret ***SK*** to privacy and authentication keys as follows. First, <u>the agent transforms the shared secret ***SK*** into a readable password of preferably16 characters (or fewer) (step 106)</u>. Preferably, this is performed by discarding any OCTETS (in the ***SK*** string) beyond the 16^{th} octet and then performing the following on each remaining octet:
>
> a.. if (octet > 0x7F), then octet = octet B 0x80; // Clear the top bit
>
> b. if (octet ≤ 0x20) octet = octet + 0x40; // Re-Map control codes
>
> c. if(octet = 0x7F) octet = octet - 1; // Re-map delete character.

Advantageously, this process of generating a readable password allows an operator at the NMS to easily enter the password (as opposed to entering the shared secret octet string).

Second, the readable password is then translated into a 16 byte key, ***KC*** (step 107).

The manager will use its random number r_2 and the agent's public value P_1 (i.e., the ***tceDCM105KickstartMyPublic*** value) to compute the shared secret ***SK*** (via the Diffie-Hellman key exchange algorithm) (step 204). This is the same shared secret ***SK*** computed by the agent. Next, the manager computes the same readable password for the "docsisProv" user from the shared secret ***SK*** (step 205), and then transforms the readable password to the value of ***KC*** (step 206) using the same process as the agent (described above in steps 106-107). The manager will then set the authentication and privacy keys for the provisioned user to the value of ***KC*** (step 207). It is to be appreciated that the Diffie-Hellman key exchange ensures that both the agent and the manager compute the same 16 character password without revealing it.

The Examiner has cited "Page 12, Col 1, lines 38-48; 'secret key' shared by users and authoritative SNMP engine; converting users keys to unique keys; proposal [2]; RFC 2274" as disclosing the second converting step of Claim 1. This section is reproduced herein below.

Page 12, column 1, lines 29-48 of Stalling disclose the following:

A user requires a 16-octet privacy key and an authentication key of length either 16 or 20 octets. For keys owned by human users, it is desirable that the user be able to employ a human-readable password rather than a bit-string key. Accordingly, RFC 2274 defines an algorithm for mapping from the user password to a 16- or 20-octet key. USM places no restriction on the password itself, but local management policies should dictate that users employ passwords that are not easily guessed.

Password to key generation is performed as follows:

1. Take the user's password as input and produce a string of length 220 octets (1,048,576 octets) by repeating the password value as many times as necessary, truncating the last value f necessary, to form the string digest0. For example, an eight-character password (23 octets) would be concatenated with itself 217 times to form digest0.
2. If a 16-octet key is desired, take the MD5 hash of digest0 to form digest1. If a 20-octet key is desired, take the SHA-1 hash of digest0 to form digest1. The output is the user's key.

The preceding is one portion of a key localization method disclosed in Stallings. In further detail, Stallings discloses a process referred to as key localization, which is "[t]he process by which a single user key is converted into multiple unique keys, one for each remote SNMP engine" (Stallings, p. 12, col. 2). As is shown in Figure 7 of Stallings, a user password is input to a hash function, which takes a hash of the expanded password string and outputs a user key. Then, for each remote SNMP engine, the user key is input to a hash function that takes a hash of the user key and the remote EngineID of the corresponding remote engine to output a localized key. That is" a single user key is mapped by means of a nonreversible one-way function (i.e., a secure hash function) into different localized keys for different authenticated engines (different agents)" (Stallings, p. 12, col. 2 to p. 13, col. 1). Stallings further discloses that "[a] localized key is defined ... as a secret key shared between a user and one authoritative SNMP engine" (Stallings, p. 12). The entire key localization method of Stalling is shown in Figure 7 thereof and can be essentially represented by the following sequence: password ->(hash)-> user key ->(hash with remote EngineID)->localized key(s).

Thus, since Figure 7 of Stalling shows the user key, and not the localized keys, being converted from a password, it is the user key which must correspond to the secret key recited in the second converting step of Claim 1, which it does NOT.

Thus, in Stallings, while a user password is converted into a user key, Stalling does NOT disclose that the user key is independent converted by both an SNMP agent and an SNMP manager, as is the secret key recited in the second converting step of Claim 1. In fact, there is no need for that in Stallings, since the user key is shared amongst a plurality of SNMP engines to allow the user key to be hashed with the respective remote engineID of each respective SNMP engine to provide a localized key for the corresponding SNMP engine.

Further, given the fact that the user key in Stallings is shared amongst a plurality of SNMP engines, the user key may be considered to be a public key, since it is commonly used by all the remote engines to generate a localized key, by hashing the user key/public key common to all remote engines with the respective unique remote engineID of each remote engine.

Accordingly, Stallings does not teach or suggest the second converting step of claim 1 being independently performed both the SNMP agent and the SNMP manager as explicitly recited in Claim 1.

Moreover, the Examiner has cited "Col 9, lines 1-10; Col 10, lines 1-10; generating password from a shared secret" as disclosing the first converting step of Claim 1. This section is reproduced herein below.

In particular, column 9, lines 1-10 of Yu disclose the following:

> The user authentication system according to the present invention has functions of inquiring the account balance and trade details, initializing the service for generating a onetime password, generating the one-time password, and verifying the one-time password in the server. As shown in FIG. 4, the authentication of an authorized user is performed using the one-time password in three steps: initializing the service when a user inserts the IC card into the terminal in order to obtain the service (step 470), generating the onetime password in the terminal (step 430), and verifying the password of the user in the server (step 450).

In particular, column 10, lines 1-15 of Yu disclose the following:

> The one-time password is generated using the secret key (secret keys for the symmetrical key cipher algorithm), shared by the IC card 100 and the server 140, and also using a random number value shared by the 5 terminal 120 and the server 140. When the user inserts the IC card 100 into the terminal 120 (step 400 of FIG. 4) and commands the terminal to generate a one-time password, the symmetrical key cipher portion 200 of the first password generator 123 in the terminal 120 reads the secret key from the IC card 100 and the random number and the counter 10 value from the random number

> memory 122 at step 610, generates a cipher from the read values using the symmetrical key cipher algorithm at step 620, and calculates the resultant binary value using a one way hash function in the hash function portion 210 at step 630.

Since Yu is directed to a "user authentication system for authenticating an authorized user of an IC card" (Yu, Title), Yu does not even mention once SNMP, let alone an SNMP agent or an SNMP manager, or further that both an SNMP agent and an SNMP manager independently convert a shared secret into a readable password as recited in Claim 1.

Accordingly, Yu does not teach or suggest the first converting step of claim 1 being independently performed both the SNMP agent and the SNMP manager as explicitly recited in Claim 1.

Additionally, it is respectfully pointed out to the Examiner that "[o]bviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so" (MPEP §2143.01, citing *In re Kahn*, 441 F.3d 977, 986 78 USPQ2d 1329, 1335 (Fed. Cir. 2006)).

A prior art reference must be considered in its entirety, i.e., as a whole, INCLUDING PORTIONS THAT WOULD LEAD AWAY FROM THE CLAIMED INVENTION. *W.L. Gore & Associates, Inc. v. Garlock, Inc.*, 721 F.2d 1540, 220 USPQ 303 (Fed Cir. 1983), *cert. denied*, 469 U.S. 851 (1984) (emphasis added) (*see also*, MPEP §2141.03)).

Thus, here it is not only respectfully asserted that no such teaching, suggestion, or motivation exists to combine and/or modify the references to produce the invention claimed in Claim 1, but further that StJohn teaches away from the proposed combination.

For example, StJohn discloses simply truncating the shared secret, without more, to match the number of bits required for the protocol, and nothing further, as the proposed combination suggested by the Examiner would require to obtain all the limitations recited in Claim 1. For example, StJohn discloses "[t]he right-most n bits of the shared secret 'sk', where 'n' is the number of bits required for the protocol defined by usmUserAuthProtocol, are installed as the operational authentication key" (StJohn, p. 8, last line to p. 9, first three lines; see also, StJohn, p. 7, third full paragraph).

Accordingly, the application of StJohn to the pending claims is NOT sufficient in the first place (as StJohns teaches away from the recited Claim limitations) and, further, neither

Stallings nor Yu cure the deficiencies of StJohn identified by the Examiner, and are silent with respect to the above recited limitations of Claim 1.

"To establish prima facie obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art" (MPEP §2143.03, citing *In re Royka*, 490 F.2d 981, 180 USPQ 580 (CCPA 1974)). Accordingly, independent Claim 1 is patentably distinct and non-obvious over the cited references for at least the reasons set forth above.

"If an independent claim is nonobvious under 35 U.S.C. 103, then any claim depending therefrom is nonobvious" (MPEP §2143.03, citing *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)).

Claims 2-7 depend from Claim 1 or a claim which itself is dependent from Claim 1 and, thus, includes all the elements of Claim 1. Accordingly, Claims 2-7 are patentably distinct and non-obvious over the cited references for at least the reasons set forth above with respect to Claim 1.

Accordingly, reconsideration of the rejections is respectfully requested.

In view of the foregoing, Applicants respectfully request that the rejection of the claims set forth in the Office Action of March 21, 2007 be withdrawn, that pending claims 1-7 be allowed, and that the case proceed to early issuance of Letters Patent in due course.

It is believed that no additional fees or charges are currently due. However, in the event that any additional fees or charges are required at this time in connection with the application, they may be charged to applicants' Deposit Account No.07-0832.

Respectfully submitted,

Patent Operations
Thomson Licensing Inc.
P.O. Box 5312
Princeton, NJ 08543-5312

By: /Guy H. Eriksen/
Guy H. Eriksen, Attorney for Applicants
Registration No.: 41,736
(609) 734-6807

May 1, 2007